



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/435,803	11/08/1999	MISAO KIMURA	FUJH-16.715	5700

26304 7590 01/21/2004

KATTEN MUCHIN ZAVIS ROSENMAN
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 01/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

3

Office Action Summary

Application No.

09/435,803

Applicant(s)

KIMURA, MISAO

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 October 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 November 1999 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____
- 4) ☐ Interview Summary (PTO-413) Paper No(s) _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. The amendment filed on 30 October 2003 is noted and made of record.
2. Claims 1 through 7 are presented for examination.

Drawings

3. Applicant is reminded that the Patent and Trademark Office no longer makes drawing changes and that it is applicant's responsibility to ensure that the drawings are corrected in accordance with the instructions set forth in Paper No. 4, mailed on 30 July 2003.

Response to Arguments

4. Applicant's arguments with respect to claims 1 through 7 have been considered but are moot in view of the new ground(s) of rejection.
5. See further rejections that follow.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1, 2, 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,402,490 to Mihm, Jr., hereinafter Mihm, in view of U.S. Patent No. 6,026,163 to Micali, hereinafter Micali.
8. As per claim 1, Mihm teaches a network system providing secure communication services, comprising:

Art Unit: 2131

central management and control equipment (Figure 1 [blocks 16, 30]; column 3, lines 31-66); and,

a plurality of pieces of switching equipment, each piece of switching equipment including an encryption section (Figure 1 [blocks 14, 16]; column 3, lines 31-66);

each piece of switching equipment being individually connected to said central management and control equipment, and said plurality of pieces of switching equipment constituting a circuit switched public network (Figure 1 [blocks 14, 16, 30]; column 3, lines 31-66); and,

9. Mihm does not teach:

wherein said central management and control equipment delivers to a piece of switching equipment accommodating a data terminal of a calling party, a public key for a piece of switching equipment accommodating a data terminal of a called party and a common key to encrypt a message for transmission via the circuit switched public network from the data terminal of the calling party to the data terminal of the called party each time a call requesting secure communication is originated from the piece of switching equipment accommodating the data terminal of the calling party.

10. Micali teaches:

wherein said central management and control equipment delivers to a piece of switching equipment accommodating a data terminal of a calling party, a public key for a piece of switching equipment accommodating a data terminal of a called party and a common key to encrypt a message for transmission via the circuit switched public network from the data terminal of the calling party to the data terminal of the called party each time a call requesting

Art Unit: 2131

secure communication is originated from the piece of switching equipment accommodating the data terminal of the calling party (Figure 1; column 2, lines 8-17; column 2, lines 28-40; claim 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the central management and control equipment provide a public key and a common key to encrypt a message between two end terminals. One would be motivated to provide for the abovementioned function as it ensures a different encryption each time a communication occurs between two terminals making it more difficult to eavesdrop. This is especially beneficial in sensitive communications, such as communications to an aircraft, ship, or satellite.

11. Regarding claim 2, Mihm teaches:

wherein said central management and control equipment has a database maintaining public keys of the plurality of pieces of switching equipment, and receives from pieces of the switching equipment having detected the call a called dial number and a user identification number assigned in said pieces of switching equipment (Figures 7, 8, 12; column 7, lines 9-23),

to retrieve in said database the public key of the piece of switching equipment accommodating the called dial number, and a public key of the piece of switching equipment detecting the originated call, using the called dial number and the user identification number (Figures 7, 8, 12; column 7, lines 9-23).

12. Mihm does not teach:

to generate the common key using the retrieved public keys.

13. Micali teaches:

Art Unit: 2131

to generate the common key using the retrieved public keys (Figure 1; column 2, lines 8-17; claim 1).

14. Regarding claim 4, Mihm teaches:

wherein said piece of switching equipment detecting the originated call is controlled so as to transit to the secure communication mode at each time of call origination (Figure 8; column 3, lines 37-56; column 9, lines 36-59).

15. Regarding claim 5, Mihm teaches:

wherein said piece of switching equipment detecting the originated call is controlled so as to transit to the secure communication mode by the detection of indication in said call requesting to transit to the secure communication mode (Figure 8; column 3, lines 37-56; column 9, lines 36-59).

16. Claims 3, 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mihm in view of Micali as applied to claim 1 above, and further in view of U.S. Patent No. 5,124,117 to Tatebayashi et al., hereinafter Tatebayashi.

17. Regarding claim 3, Mihm and Micali do not teach

wherein said piece of switching equipment having detected the originated call encrypts the common key delivered from the central management and control equipment, using the public key of the piece of switching equipment accommodating the called party, to forward to said piece of switching equipment accommodating the called party,

Art Unit: 2131

thereby said piece of switching equipment accommodating the called party decrypts the encrypted common key received from the switching equipment having detected the originated call, using a private key maintained in said piece of switching equipment accommodating the called party.

18. Tatebayashi teaches:

wherein said piece of switching equipment having detected the originated call encrypts the common key delivered from the central management and control equipment, using the public key of the piece of switching equipment accommodating the called party, to forward to said piece of switching equipment accommodating the called party (column 9, lines 24-62),

thereby said piece of switching equipment accommodating the called party decrypts the encrypted common key received from the switching equipment having detected the originated call, using a private key maintained in said piece of switching equipment accommodating the called party (column 9, lines 24-62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the common key. One would be motivated to encrypt the common key as to keep it hidden from unauthorized users, because if the common key became known it would be easy to crack any message from a user that contributed to the common key.

19. As per claim 6, Mihm teaches a method for delivering an encryption key to enable secure communication in a communication system having central management and control equipment and a plurality of pieces of switching equipment, each of said pieces of switching equipment including an encryption section, and each piece of switching equipment being individually

Art Unit: 2131

connected to said central management and control equipment, and said plurality of pieces of switching equipment constituting a circuit switched public network, the method comprising the steps of:

informing the central management and control equipment from a piece of switching equipment detecting a call data terminal, which is accommodated by said switching equipment, of a called number of a called data terminal and a user identification number assigned to the pieces of switching equipment detecting the calling data terminal (Figures 1 [blocks 16, 30], 10, 11; column 3, lines 31-66; column 10, line 64 to column 11, line 29);

retrieving in a database of the central management and control equipment a public key for a piece of switching equipment accommodating the called data terminal using the called number of the called data terminal (Figures 7, 8, 12; column 7, lines 9-23; column 11, lines 12-29).

20. Mihm does not teach:

generating a common key using the retrieved public key for the piece of switching equipment accommodating the called data terminal and a public key for the piece of switching equipment detecting the calling data terminal;

encrypting in the piece of switching equipment detecting the calling data terminal, the generated common key using the retrieved public key of the piece of switching equipment accommodating the called party;

forwarding the encrypted common key to said piece of switching equipment accommodating the called party via the circuit switched public network; and,

Art Unit: 2131

regenerating the encrypted common key in the piece of switching equipment accommodating the called party using a private key of said switching equipment accommodating the called party.

21. Micali teaches:

generating a common key using the retrieved public key for the piece of switching equipment accommodating the called data terminal and a public key for the piece of switching equipment detecting the calling data terminal (Figure 1; column 2, lines 8-17; column 2, lines 28-40; claim 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the central management and control equipment provide a public key and a common key to encrypt a message between two end terminals. One would be motivated to provide for the abovementioned function as it ensures a different encryption each time a communication occurs between two terminals making it more difficult to eavesdrop. This is especially beneficial in sensitive communications, such as communications to an aircraft, ship, or satellite.

22. Tatebayashi teaches:

encrypting in the piece of switching equipment detecting the calling data terminal, the generated common key using the retrieved public key of the piece of switching equipment accommodating the called party (column 9, lines 24-62);

forwarding the encrypted common key to said piece of switching equipment accommodating the called party via the circuit switched public network (column 9, lines 24-62); and,

Art Unit: 2131

regenerating the encrypted common key in the piece of switching equipment accommodating the called party using a private key of said switching equipment accommodating the called party (column 9, lines 24-62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the common key. One would be motivated to encrypt the common key as to keep it hidden from unauthorized users, because if the common key became known it would be easy to crack any message from a user that contributed to the common key.

23. Regarding claim 7, Mihm teaches further comprising the step of:

encrypting a called number and a user identification number assigned in a piece of switching equipment detecting the call using a public key of the central management and control equipment, to transfer from said piece of switching equipment detecting the call to said central management and control equipment (Figures 7, 8, 12; column 7, lines 9-23; column 8, lines 9-19).

Conclusion

24. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

25. A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period

Art Unit: 2131

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704.

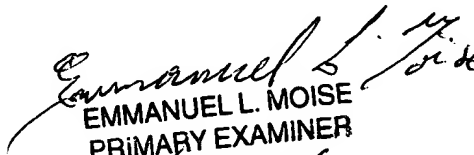
The examiner can normally be reached on Monday thru Thursday 7-5.

27. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7240.

28. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf


EMMANUEL L. MOISE
PRIMARY EXAMINER
A/11 2136